

# A congruence sum and rational approximations

Sandro Bettin

January 25, 2017

## Abstract

We give a reciprocity formula for a two-variable sum where the variables satisfy a linear congruence condition. We also prove that such sum is a measure of how well a rational is approximable from below and show that the reciprocity formula is a simple consequence of this fact.

## 1 A congruence sum

Sums over the integers subject to some congruence conditions are ubiquitous in number theory and often appear in several other areas of mathematics. They are related to many classical arithmetic problems (e.g. that of primes in arithmetic progression, the Dirichlet's divisor problem, etc.) and even when they seem particularly innocuous there is actually a lot of arithmetic information hidden in them. This is the case of the sum

$$S(a/q) := \sum_{\substack{am \equiv n \pmod{q}, \\ mn < q, \ n, m > 0}} 1,$$

where  $a, q \in \mathbb{Z}$ ,  $q > 0$ , and  $(a, q) = 1$ , which counts the number of points  $(m, n)$  in  $(\mathbb{Z}/q\mathbb{Z})^2$  which belong to the line  $am \equiv n \pmod{q}$  and are contained in the hyperbolic region  $mn < q$  (here of course we mean the representatives with  $0 < m, n \leq q$ ). Notice that  $S$  can be interpreted as a 1-periodic function defined over the rational numbers.

Two “visual” examples of such function are given in Figure 1 below. Notice that in both cases  $S(-226, 307) = S(307, 226) = 7$  and the two graphs look overall very similar. This is actually not a coincidence: indeed one always have that  $S(-a, q)$  is close to  $S(q, a)$  (for  $q = 307$  their difference is always  $\leq 3$  and is typically either 0 or 1, whereas the maximum value of  $S(a, 307)$  is 17). A similar relation holds for  $S(a, q)$  and  $S(-q, a)$ , with the difference that in this case one also has a main term. These two facts are expressed in the following theorem.

**Theorem 1.** *Let  $1 \leq a < q$ . Then,*

$$S(a/q) - S(-q/a) = \sqrt{q/a} + E_+(a, q), \quad (1.1)$$

$$S(-a/q) - S(q/a) = E_-(a, q), \quad (1.2)$$

with  $|E_{\pm}(a, q)| \leq \frac{3}{2}k_{a/q} + 3$  where  $k_{a/q}$  is the number of steps in the Euclid division  $q/a$  (in particular  $E_{\pm}(a, q) \ll \log(2 + q)$ ).

---

2010 *Mathematics subject classification.* 11A55 (primary), 11A07, 11A15, 11N37, 11J70 (secondary)  
*Key words and phrases.* Congruence sum; rational approximation, continued fractions.

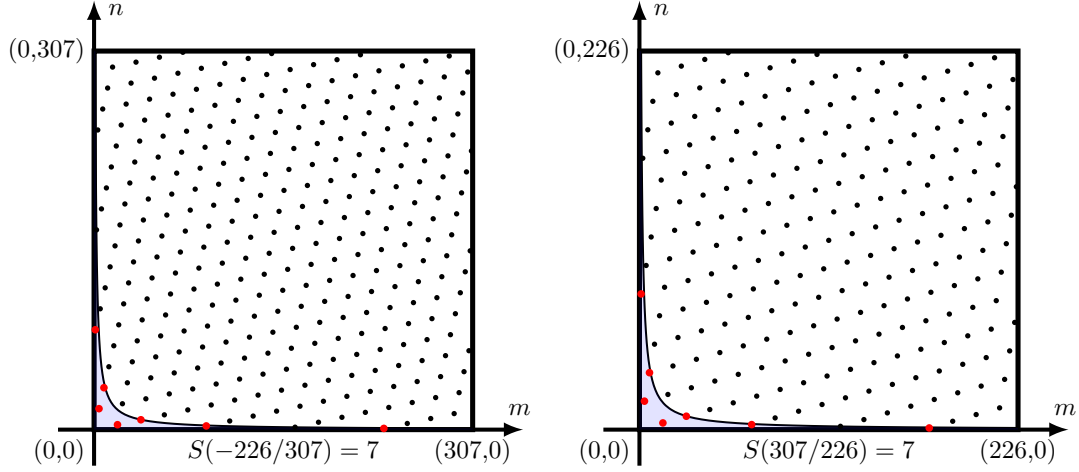


Figure 1: A visual computation of  $S(a/q)$  in the case  $(a, q) = (-226, 307)$  and  $(a, q) = (307, 226)$ . The points represent the couples  $(m, n) \in \{0 < r < q\}^2$  satisfying  $am \equiv n \pmod{q}$ , the red ones being the ones below the hyperbola  $mn = q$ .

The  $\leq$  part of these inequalities was already obtained by Young [You] in his extension of Conrey's reciprocity formula for the twisted second moment of Dirichlet  $L$ -functions [Con]. Young also obtained a similar version of these formulas in the case when the sharp cut-off  $mn \leq q$  is replaced by a smooth one, that is by inserting a factor of  $f(mn/q)$  where  $f(x)$  is a smooth function going to zero faster than any polynomial at  $+\infty$  (see also [Bet15] for an alternative treatment of the smoothed case). We remark that the same method used to prove Theorem 1 can be used to obtain a simpler proof of the Conrey-Young reciprocity formula for the twisted second moment.

Theorem 1 suggests that one can obtain a formula for  $S(a/q)$  in terms of the coefficients of the continued fraction expansion  $[0; b_1, \dots, b_k]$  of  $a/q$ . Indeed one can repeatedly alternate the use of one among (1.1) or (1.2) and the reduction modulo the denominator and obtain

$$S(a/q) = \sum_{j=0}^{\lfloor (k-1)/2 \rfloor} \sqrt{b_{2j+1}} + O(k_{a/q}^2).$$

However, in fact one can prove directly a stronger form of this result, with  $O(k_{a/q}^2)$  replaced by  $O(k_{a/q})$ , and then deduce Theorem 1 from it.

**Theorem 2.** *Let  $a, q \in \mathbb{Z}$  with  $q > 0$ ,  $a \neq 0$  and  $(a, q) = 1$ . Let  $[0; b_1, \dots, b_k]$  be the continued fraction expansion of  $\frac{a}{q}$ . Then*

$$S(a/q) = \sum_{j=0}^{\lfloor (k-1)/2 \rfloor} [\sqrt{b_{2j+1}}] + E,$$

where  $0 \leq E \leq \frac{3}{2}k + 1 \ll \log(2 + q)$  and  $[x]$  denotes the integer part of  $x$ .

Theorem 2 doesn't provide a useful asymptotic formula for most values of  $a$ . Indeed, a standard (but somewhat lengthy) computation with Dirichlet's hyperbola method shows that the average

value of  $S(a/q)$  is

$$\frac{1}{\varphi(q)} \sum_{\substack{0 < a < q, \\ (a,q)=1}} S(a/q) = \frac{\varphi(q)\sigma_{-1}(q)}{q} (\log q + O(\log \log q)) \asymp \log q,$$

as  $q \rightarrow \infty$ , where  $\sigma_{-1}(q) = \sum_{d|q} d^{-1}$  and  $\varphi$  is Euler's totient function.<sup>1</sup> However, Theorem 2 is still useful as it determines exactly all the large values of  $S(a/q)$ . Indeed, the Theorem shows that  $S(a/q)$  is “large” if and only if the continued fraction expansion of  $a/q$  has a “large” odd coefficient.

Theorem 2 can also be used to prove some density results for  $S(a/q)$ , following the method introduced by Hickerson [Hic] for the Dedekind sum. For example, we can prove the following.

**Corollary 1.** *Let  $\kappa > 1$ . Then the set  $\left\{ \left( \frac{a}{q}, \frac{S(a/q)}{\log^\kappa(2+q)} \right) \mid \frac{a}{q} \in \mathbb{Q} \right\}$  is dense in  $\mathbb{R} \times \mathbb{R}_{>0}$ .*

It would be interesting to understand how the set  $\{(\frac{a}{q}, S(a/q)) \mid \frac{a}{q} \in \mathbb{Q}\}$  is distributed as  $q \rightarrow \infty$  (see [Var] and [Bet15] for the computation of the distribution of two somewhat similar sums via the use of reciprocity formulas close to (1.1) and (1.2)).

## 2 Rational approximations

Theorem 1 and 2 actually admit a rather simple explanation, once one realizes that  $S(a/q)$  can be defined also in another simple and apparently unrelated way. Indeed,  $S(a/q)$  coincides with the number of ways  $a/q$  can be “well approximated” from below by fractions of smaller denominator. The theory of continued fractions tells us that “good approximations” of a real number are obtained by its convergents, which then explains why the coefficients of the continued fraction expansion arise in Theorem 2.

Before stating the precise result, we give an example for the case of  $S(-226/307)$  considered in Figure 1. The 7 points  $(m, n)$  appearing in the sum defining  $S(-226/307)$  are  $(235, 1)$ ,  $(91, 3)$ ,  $(19, 4)$ ,  $(38, 8)$ ,  $(4, 17)$ ,  $(8, 34)$ ,  $(1, 81)$ . Now, compare them with the fractions  $r/s$  with  $s < 307$  which satisfy  $0 < -\frac{226}{307} - \frac{r}{s} < \frac{1}{s^2}$ . These are the even convergents  $-\frac{1}{1}$ ,  $-\frac{3}{4}$ ,  $-\frac{14}{19}$ , the “double” of the last two  $-\frac{6}{8}$ ,  $-\frac{28}{38}$ , and two of the semi-convergents  $-\frac{67}{91}$  and  $-\frac{173}{235}$ . Notice that the denominators of such fractions are precisely the  $m$ -coordinates of the 7 points! The following simple theorem tells us that this is no coincidence.

**Theorem 3.** *Let  $a, q \in \mathbb{Z}$ , with  $q > 0$  and  $(a, q) = 1$ . Then,*

$$S(a/q) = \#\{(c, d) \in \mathbb{Z}^2 \mid d > 0, 0 < \frac{a}{q} - \frac{c}{d} < \frac{1}{d^2}\}. \quad (2.1)$$

*Proof of Theorem 3.* Let  $0 < n, m < q$  with  $am \equiv n \pmod{q}$ . Let  $r$  be the largest integer such that  $\frac{r}{m} < \frac{a}{q}$ ; clearly  $0 < \frac{a}{q} - \frac{r}{m} < \frac{1}{m}$ . Also,

$$am = q \frac{a}{q} m = q \left( \frac{r}{m} + \frac{a}{q} - \frac{r}{m} \right) m \equiv q \left( \frac{a}{q} - \frac{r}{m} \right) m \pmod{q}. \quad (2.2)$$

Thus, since  $0 < q(\frac{a}{q} - \frac{r}{m})m < q$ , we must have  $q(\frac{a}{q} - \frac{r}{m})m = n$ . We then have that  $mn < q$  if and only if  $q(\frac{a}{q} - \frac{r}{m})m^2 < q$  and thus if and only if  $(\frac{a}{q} - \frac{r}{m}) < \frac{1}{m^2}$ . Thus, we obtain the  $\leq$  side of (2.2); it is clear that repeating the same argument in the opposite direction yields the other inequality and so the proof is completed.  $\square$

<sup>1</sup>Notice that if  $q$  is prime, then the average of  $S(a/q)$  reduces exactly to the Dirichlet's divisor problem:  $\frac{1}{\varphi(q)} \sum_{0 < a < q, (a,q)=1} S(a/q) = \sum_{n < q} d(n)$ , where  $d(n)$  is the number of divisors of  $n$ .

Notice that the set on the right hand side of (2.1) doesn't have the condition  $(c, d) = 1$ , that is we are not requiring the fractions  $\frac{c}{d}$  to be in reduced form. If one wants to count only reduced fractions, then one immediately sees that  $S(a/q)$  corresponds to a weighted sum, where the weight takes into account how good the approximation is:

$$S(a/q) = \sum_{\substack{(c,d)=1, d>0 \\ 0 < \frac{a}{q} - \frac{c}{d} \leq \frac{1}{d^2}}} [\varepsilon_{c/d}^{-\frac{1}{2}}], \quad (2.3)$$

where  $\varepsilon_{c/d} = d^2 |\frac{a}{q} - \frac{c}{d}|$ . The theory of continued fractions then helps us recover Theorem 2 from (2.3) and Theorem 1 will then follow easily.

Before proving the various results we make one last remark. If in  $S(a/q)$  we add the condition  $(m, n) = 1$  and include also the solutions of  $am \equiv -n \pmod{q}$ , then we have the following analogue of Theorem 3:

$$\sum_{\substack{am \equiv \pm n \pmod{q}, \\ mn < q, n, m > 0, \\ (m, n) = 1}} 1 = \#\left\{ \frac{c}{d} \in \mathbb{Q} \mid (c, d) = 1, 0 \neq \left| \frac{a}{q} - \frac{c}{d} \right| < \frac{1}{d^2} \right\} \quad (2.4)$$

valid for  $q$  prime (if  $q$  is not prime one has to add the condition  $(q, d) = 1$  in the set on the right hand side). Now, using Möbius inversion formula and the asymptotic for Dirichlet's divisor problem, we have that for  $q$  prime the average value of the left hand side is

$$\frac{1}{\varphi(q)} \sum_{\substack{a \pmod{q}, \\ (a, q) = 1}} \sum_{\substack{am \equiv \pm n \pmod{q}, \\ mn < q, n, m > 0, \\ (m, n) = 1}} 1 = \frac{12}{\pi^2} \log q + O(1),$$

as  $q \rightarrow \infty$ . Also, it is known (cf. the next Section) that all the convergents to  $\frac{a}{q}$  (different from  $\frac{a}{q}$ ) are contained in the set of the right hand side of (2.4) and that, on average over  $a$ , there are asymptotically  $\frac{12 \log 2}{\pi^2} \log q$  convergents of  $\frac{a}{q}$  as  $q$  goes to infinity among primes [Hei]. In particular, on average over  $a$  and as  $q \rightarrow \infty$  among primes, we have that  $\log 2 \approx 69.3\%$  of the solutions to  $|\frac{a}{q} - \frac{c}{d}| < \frac{1}{d^2}$  are partial quotients of  $\frac{a}{q}$ , whereas  $\approx 30.7\%$  are not. (In Lemma 2 below we will see that these other solutions are certain semi-convergents of  $a/q$ ).

We conclude this section by observing that the second moment of  $S(a/q)$  is very closely related to the 4-th moment of Dirichlet L-functions at the central point. In particular, Theorem 3 opens an alternative approach to this problem via methods of Diophantine approximation (see also [CK]).

### 3 Proofs of Theorems 2 and 1 and of Corollary 1

*Proof of Theorem 2.* It is well known (see [Khi], Chapter 1) that all convergents  $h_j/k_j$  of  $a/q$  (with  $\frac{h_j}{k_j} \neq \frac{a}{q}$ ) satisfy

$$\frac{1}{k_j(k_{j+1} + k_j)} < \left| \frac{h_j}{k_j} - \frac{a}{q} \right| < \frac{1}{k_j k_{j+1}} < \frac{1}{k_j^2}$$

and that one has  $\frac{h_j}{k_j} < \frac{a}{q}$  if and only if  $j$  is even, so that all the even convergents appear in the sum (2.3). Also, the above inequalities give

$$\frac{k_j}{(k_{j+1} + k_j)} < \varepsilon_{h_j/k_j} < \frac{k_j}{k_{j+1}}$$

and so, since  $k_{j+1} = b_{j+1}k_j + k_{j-1}$  and  $0 \leq k_{j-1} < k_j$  for  $j \geq 0$ , we obtain  $b_{j+1} \leq \varepsilon_{h_j/k_j}^{-1} \leq b_{j+1} + 2$ .

By the inequality  $[\sqrt{x+2}] - [\sqrt{x}] \leq 1$  for  $x \geq 1$  we then have  $[b_{j+1}^{\frac{1}{2}}] \leq [\varepsilon_{h_j/k_j}^{-\frac{1}{2}}] \leq [b_{j+1}^{\frac{1}{2}}] + 1$ .

The solutions  $c/d$  to  $0 < |\frac{c}{d} - \frac{a}{q}| < \frac{1}{d^2}$  are not all convergents of  $a/q$ , however this is not far from being true. Indeed, all solutions  $c/d$  with  $(c, d) = 1$  of the stricter inequality  $0 < |\frac{c}{d} - \frac{a}{q}| < \frac{1}{2d^2}$  are convergents (see [Khi], Theorem 19), so that  $|\varepsilon_{c/d}|^{-1} \leq 2$  if  $c/d$  is not a convergent. In particular, (2.3) gives

$$S(a/q) = \sum_{\substack{j=1, \\ j \text{ odd}}}^k [b_j^{\frac{1}{2}}] + S^*(a/q) + \mathcal{E}_{a,q}$$

where  $0 \leq \mathcal{E}_{a,q} \leq (k+1)/2$  and  $S^*(a/q)$  is the number of reduced rationals  $c/d$  satisfying  $0 < \frac{a}{q} - \frac{c}{d} < \frac{1}{d^2}$  which are not convergents of  $a/q$ . By Lemma 2 below  $S^*(a/q)$  is bounded by twice the number of even convergents of  $\frac{a}{q}$  (different from  $a/q$ ), so that  $S^*(a/q) \leq k$  and the proof of Theorem 2 is completed.  $\square$

**Lemma 2.** *Let  $\frac{a}{q} \in \mathbb{Q}$  with continued fraction expansion  $[b_0; b_1, \dots, b_k]$  and convergents  $\frac{h_j}{k_j}$  for  $-1 \leq j \leq k$ . Then, every  $\frac{c}{d} \in \mathbb{Q}$  which satisfies  $0 \neq |\frac{a}{q} - \frac{c}{d}| < \frac{1}{d^2}$  with  $(c, d) = 1$  is either a convergent  $\frac{h_j}{k_j}$  of  $\frac{a}{q}$  (with  $-1 \leq j \leq k-1$ ) or a semi-convergent of the form  $\frac{h_j + gh_{j+1}}{k_j + gk_{j+1}}$  with  $g = 1$  or  $g = b_{j+2} - 1$  (and  $-1 \leq j \leq k-2$ ). Moreover, in both cases  $c/d < a/q$  if and only if  $j$  is even.*

*Proof.* We assume  $\frac{a}{q} < \frac{c}{d}$ , the proof being essentially identical otherwise. Now, if  $0 < \frac{a}{q} - \frac{c}{d} < \frac{1}{d^2}$  with  $(c, d) = 1$ , then  $\frac{c}{d}$  is a “best rational approximation from below” for  $a/q$ , that is  $\frac{c}{d}$  is closer to  $\frac{a}{q}$  than any rational which is less than  $a/q$  and have a smaller denominator. Indeed, if  $0 < d' < d$  and  $0 < \frac{a}{q} - \frac{c'}{d'} \leq \frac{a}{q} - \frac{c}{d}$  for some  $c' \in \mathbb{Z}$ , then

$$\frac{1}{dd'} \leq \frac{c'}{d'} - \frac{c}{d} \leq \left( \frac{a}{q} - \frac{c}{d} \right) - \left( \frac{a}{q} - \frac{c'}{d'} \right) < \frac{1}{d^2}$$

which gives a contradiction. Now, all the best rational approximation from above or below for  $\frac{a}{q}$  which are not convergents are semi-convergents of the form  $\frac{h_j + gh_{j+1}}{k_j + gk_{j+1}}$  for  $g$  an integer satisfying  $1 \leq g < b_{j+2}$  (Theorem 15 of [Khi] proves this for best rational approximations, but the proof carries over also for best approximations from below or from above); also this fraction is smaller than  $\frac{a}{q}$  if and only if  $j$  is even. We will now show that among these only the values  $g = 1$  and  $g = b_{j+2} - 1$  might be such that the inequality  $|\frac{h_j + gh_{j+1}}{k_j + gk_{j+1}} - \frac{a}{q}| < \frac{1}{(k_j + gk_{j+1})^2}$  is satisfied.

Clearly we can assume  $b_{j+2} \geq 4$ , since otherwise there is nothing to prove. For  $j$  even we have  $k_{j+1}h_j - k_jh_{j+1} = 1$  and so

$$\frac{h_{j+2}}{k_{j+2}} - \frac{h_j + gh_{j+1}}{k_j + gk_{j+1}} = \frac{b_{j+2} - g}{(k_j + b_{j+2}k_{j+1})(k_j + gk_{j+1})}.$$

Since  $\frac{h_j + gh_{j+1}}{k_j + gk_{j+1}} < \frac{h_{j+2}}{k_{j+2}} \leq \frac{a}{q}$ , then it follows that in order to have  $\frac{a}{q} - \frac{h_j + gh_{j+1}}{k_j + gk_{j+1}} < \frac{1}{(k_j + gk_{j+1})^2}$  it is necessary that

$$(b_{j+2} - g)(k_j + gk_{j+1}) < (k_j + b_{j+2}k_{j+1}).$$

and a fortiori one must have  $(b_{j+2} - g)g < b_{j+2}$ , since  $b_{j+2} - g \geq 1$ . Solving for  $g$  we obtain

$$g < \frac{b_{j+2} - \sqrt{b_{j+2}^2 - 4b_{j+2}}}{2} \quad \text{or} \quad g > \frac{b_{j+2} + \sqrt{b_{j+2}^2 - 4b_{j+2}}}{2}$$

and thus, reminding that  $g$  is a positive integer greater than or equal to 2, the only possibilities are  $g = 1$  and  $g = b_{j+2} - 1$ , as desired.  $\square$

*Proof of Theorem 1.* A simple computation shows that if  $a/q = [b_0; b_1, b_2, \dots, b_k]$  with  $b_0 \geq 0$  and  $a \neq 0$ , then the continued fraction expansion of  $-\frac{q}{a}$  is

$$-\frac{q}{a} = \begin{cases} [-b_1 - 1; 1, b_2 - 1, b_3, b_4, \dots, b_k] & \text{if } b_2 = 1, \\ [-b_1 - 1; b_3 + 1, b_4, b_5, \dots, b_k] & \text{if } b_2 > 1, \end{cases} \quad (3.1)$$

if  $b_0 = 0$  and  $k \geq 2$  (if  $k = 1$  then  $-\frac{q}{a} = -b_1$ ) and

$$-\frac{q}{a} = \begin{cases} [-1; 1, b_0 - 1, b_1, b_2, \dots, b_k] & \text{if } b_0 = 1, \\ [-1; b_1 + 1, b_2, b_3, \dots, b_k] & \text{if } b_0 > 1, \end{cases} \quad (3.2)$$

if  $b_0 > 0$  (if  $k = 0$  and  $b_0 = 1$  then  $-\frac{q}{a} = -1$ ). Equation (1.1) then follows from (3.1) and Theorem 2 upon observing that  $b_1 \leq q/a < b_1 + 1$  and thus  $[\sqrt{b_1}] \leq \sqrt{q/a} < [\sqrt{b_1}] + 1$ . Equation (1.2) follows in the same way from (3.2) exchanging the roles of  $a$  and  $q$ .  $\square$

*Proof of Corollary 1.* Let  $(x, y) \in \mathbb{R} \times \mathbb{R}_{>0}$ . For every fixed  $\varepsilon > 0$  we need to find  $a/q$  such that  $|a/q - x| < \varepsilon$  and  $|S(a/q)/\log^\kappa(2 + q) - y| < \varepsilon$ . Since  $S(a/q)$  is 1-periodic, we can assume  $0 < x < 1$ . Let  $b_1, \dots, b_{2r}$  be such that  $|x - [0; b_1, \dots, b_{2r}]| \leq \varepsilon/2$  for some  $r \ll_\varepsilon 1$ . For  $m, n \in \mathbb{N}$ , let  $\frac{a}{q} = [0; b_1, \dots, b_{2r}, m, n]$  so that  $q = (dm + d')n + d$  for some  $d, d' \ll 1$  (considering  $b_1, \dots, b_{2r}, x, y, r$  as fixed). Thus, by Theorem 2, we have

$$\frac{S(a/q)}{\log^\kappa(2 + q)} = \frac{\sqrt{m}}{\log^\kappa(2 + mn)} + o(1).$$

as  $m, n \rightarrow \infty$ . We take  $n = \lceil e^{m^{\frac{1}{2\kappa}} y^{-\frac{1}{\kappa}}} \rceil$  and the Corollary follows by taking  $m$  large enough.  $\square$

## Acknowledgement

This note was mostly written while the author was a postdoctoral fellow at the Centre de recherches mathématiques in Montréal.

## References

- [Bet15] Bettin, S. *On the distribution of a cotangent sum*. Int Math Res Notices (2015) 2015 (21): 11419–11432.
- [Bet16] Bettin, S. *On the reciprocity law for Dirichlet L-functions*. Trans. Amer. Math. Soc. 368 (2016), 6887–6914.
- [Con] Conrey, J.B. *The mean-square of Dirichlet L-functions*. arxiv math.NT/0708.2699.

- [CK] Conrey, J.B.; Keating, J.P. *Moments of Zeta and Correlations of Divisor-Sums: II*. Advances in the Theory of Numbers. Volume 77 of the series Fields Institute Communications pp. 75–85.
- [Hei] Heilbronn, H. *On the average length of a class of finite continued fractions*. 1969 Number Theory and Analysis (Papers in Honor of Edmund Landau) pp. 87–96 Plenum, New York
- [Hic] Hickerson, D. *Continued fractions and density results for Dedekind sums*. J. Reine Angew. Math. 290 (1977), 113–116.
- [Khi] Khinchin, A.Y. *Continued fractions*. The University of Chicago Press, Chicago, Ill.-London 1964.
- [Var] Vardi, I. *Dedekind sums have a limiting distribution*. Int Math Res Notices (1993) 1993 (1): 1–12.
- [You] Young, M.P. *The reciprocity law for the twisted second moment of Dirichlet L-functions*. Forum Math. 23 (2011), no. 6, 1323–1337.

S. Bettin, DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DI GENOVA; VIA DODECANESO 35; 16146 GENOVA; ITALY.  
*E-mail address:* `bettin@dimma.unige.it`